DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
FORT KNOX, KENTUCKY 40121-5000

REPLY TO
ATTENTION OF:

Expires 27 October 2007

IMSE-KNX-IM (25)   27 October 2005

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: USAARMC Policy Memo No. 10-05 – Computer Administrative Rights

1. References.

    a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

    b. AR 25-2, Information Assurance, 14 November 2003.

2. Purpose. The Fort Knox Automated Information Systems (i.e., laptops, desktops, servers, and Campus Area Network) infrastructure provides the primary automated information infrastructure supporting operational and administrative functions. These systems provide reliable, timely, and direct methods of communicating electronically and storing information essential to daily operations. Technical controls must be adopted to ensure that access to information resources is limited to authorized personnel.

3. Applicability. This policy applies to all Soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to the Fort Knox Campus Area Network.

4. Policy. Administrative privileges are defined as membership in the domain's local administrator group or the Fort Knox Operator group.

    a. Administrative privileges will **NOT** be granted based on an individual's rank or position.

    b. The installation Information Assurance Manager (IAM) is the approval authority for granting administrator privileges.

    c. Requests for individuals requiring administrator privileges must be signed by the unit commander/director and sent to the installation IAM. The user will not receive administrator privileges until the unit commander/director receives an approval from the installation IAM.

    d. Administrator privileges shall be granted only to individuals who meet the following criteria:

(1) The majority of the individual's primary duties consist of installing, configuring, maintaining and managing the hardware, software, communications, and security of network resources and the individual must be appointed as an Information Management Officer (IMO) or Information Assurance Security Officer (IASO).

(2) The individual meets the educational requirements through the use of computer-based training, CDs, classroom instruction, or a combination of all three.

(a) Required Training. IASO Technical Training Course, IASO Management Course, and Information Assurance User Awareness Training.

(b) Copies of training certificates must be provided to the installation IAM, unit training officer, and administrative staff as appropriate.

e. The individual must be in an Information Technology (IT) II sensitivity position. This applies to any individual with the ability to change system security configurations.

f. Limited rights may be granted to users who are determined by the IAM to require power user status for the administration of specific applications. This will be determined on a case-by-case basis.

FOR THE COMMANDER:

MARK NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A

CF:
DCG, USAARMC